Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ȘI SECURITATE

Nr. 1 (160) / 2019
Indexat în CEEOL

MEDIUL VIRTUAL ȘI LEGISLAȚIA DE DREPT INTERNAȚIONAL A CONFLICTELOR ARMATE – *JUS IN BELLO*

Bogdan-Florin TIMIȘ

Virtual environment and international law of armed conflict – jus in bello

Abstract: *"Jus in bello" regulates the behaviour of the parties involved in an armed conflict. Synonymous with "jus in bello" is the international humanitarian law, hereinafter referred to as IHL, which has as its primary purpose not to prohibit armed conflicts themselves but to minimize the suffering caused by them, in particular by establishing rules for the protection of certain categories of persons, objects and activities during their development. Considering the destructive potential of cyber-attacks, sensed since the emergence of this new environment for executing such actions - the virtual environment - questions arise as to the applicability of IHLs to cyber operations in the context of armed conflict.*

Keywords: *cyber space, cyber war, legislation, armed conflict.*

Mediul virtual și legislația de drept internațional a conflictelor armate – jus in bello

Rezumat: *„Jus in bello" reglementează comportamentul părților implicate într-un conflict armat. Sinonim cu „jus in bello" este dreptul internațional umanitar, denumit în continuare DIU, care are ca scop primordial nu interzicerea conflictelor armate în sine, ci minimizarea suferințelor cauzate de acestea, în special prin instituirea unor reguli de protecție a anumitor categorii de persoane, obiecte și activități pe timpul desfășurării acestora. Având în vedere potențialul distructiv al atacurilor cibernetice, intuit încă de la apariția acestui nou mediu de executare a unor astfel de acțiuni - mediul virtual -, s-au ridicat întrebări cu privire la aplicabilitatea DIU în operațiile cibernetice desfășurate în contextul ducerii unui conflict armat.*

Cuvinte-cheie: *spațiu cibernetic, război cibernetic, legislație, conflict armat.*

Introducere

Trebuie precizat încă de la început faptul că nu vom găsi menţiuni exprese referitoare la războiul cibernetic sau la modul de executare a operaţiilor cibernetice nici în Convenţiile de la Geneva[1] şi nici în Protocoalele adiţionale[2], dar este clar că principiile şi regulile din aceste acorduri internaţionale care tratează mijloacele şi metodele de război nu se limitează doar la situaţiile care existau la momentul adoptării lor. De altfel, dreptul internațional umanitar (DIU) a anticipat progresele tehnologice şi dezvoltarea unor noi mijloace şi metode de ducere a războaielor, în sensul în care, deși nicio regulă expresă a cadrului normativ al conflictelor armate nu reglementează activităţile cibernetice, există *clauza Martens* care stipulează că: *„Până când va putea fi elaborat un cod mai complet al legilor războiului, Înaltele Părţi contractante socotesc oportun să constate că, în cazurile necuprinse printre dispoziţiile reglementare, adoptate de ele, populaţiile şi beligeranţii rămân sub garanţia şi sub imperiul principiilor Dreptului ginţilor, aşa cum rezultă ele din obiceiurile fixate între naţiunile civilizate, din legile omeniei şi din cerinţele conştiinţei publice*"[3].

Simplul fapt că un atac cibernetic, în sine, nu este fizic sau violent, nu înseamnă că depăşeşte sfera de competenţă a DIU. Ca şi în cazul altor mijloace şi metode de război, operaţiile cibernetice executate împotriva combatanţilor şi obiectivelor mili-

Bogdan-Florin TIMIȘ, *consilier juridic în Ministerul Apărării Naționale, este doctorand în domeniul Științe Militare în cadrul Universității Naționale de Apărare „Carol I" din București (e-mail: bog_timis@yahoo.com).*

tare sunt legale doar dacă sunt compatibile cu prevederile DIU. În acest context, principiul de bază care trebuie luat în calcul şi care oferă îndrumare omenirii când aceasta se confruntă cu apariţia unor noi metode şi mijloace de război este principiul potrivit căruia civilii, mijloacele lor de trai şi mediul în care aceştia trăiesc trebuie să fie protejate.

Primele situaţii celebre în care putem vorbi despre modalitatea aplicării legislaţiei conflictelor armate în cazul folosirii operaţiilor cibernetice au fost cele din Estonia, în 2007, şi Georgia, în 2008. Totuși, deşi Estonia a fost ţinta unor operaţii cibernetice asidue, apreciez că nu putem pune în discuţie aplicarea legislaţiei conflictelor armate de vreme ce situaţia nu a escaladat la nivelul unui conflict armat. În schimb, întrucât între Georgia şi Rusia era în desfăşurare un conflict armat internaţional, cadrul normativ al conflictelor armate trebuia aplicat şi în situaţia operaţiilor cibernetice. Aşadar, în cazul unor ostilităţi fizice care întrunesc condiţiile unui conflict armat, cu caracter internaţional sau non-internaţional, legislaţia conflictelor armate va guverna inclusiv modalitatea în care vor fi executate operaţiile cibernetice în cadrul respectivului conflict. De asemenea, trebuie precizat faptul că, în general, respectarea legislaţiei internaționale a conflictelor armate este obligatorie indiferent de calificarea situaţiei din perspectiva încălcării preliminare a principiilor și regulilor de „jus ad bellum", adică şi în cazul unei recurgeri ilegale la forţă.

Fireşte, aplicarea cadrului normativ al conflictelor armate în executarea operaţiilor cibernetice este problematică. De cele mai multe ori, este extrem de dificil să se identifice atacatorul, obiectivul, efectele sau chiar operaţia cibernetică în sine. Cu toate aceste dificultăţi, necesitatea respectării legislaţiei conflictelor armate în dezvoltarea operaţiilor cibernetice nu trebuie pusă sub semnul întrebării. În măsura în care operaţiile cibernetice sunt desfăşurate în cadrul unui conflict armat, *clauza Martens*, care reflectă dreptul internaţional cutumiar, intră în acţiune ca o asigurare că astfel de operaţii nu se desfăşoară într-un vid legislativ.

1. Contextul geografic în operaţiile cibernetice

Legislaţia conflictelor armate, împreună cu alte domenii ale dreptului internaţional, detaliază spaţiul geografic în care se pot desfăşura operaţiile militare, inclusiv cele cibernetice. Aspectele legale relevante tratează locul din care sunt lansate operaţiile, locaţia oricăror altor instrumente necesare operaţiilor şi zona în care sunt amplasate infrastructurile cibernetice vizate.

De regulă, operaţiile cibernetice ale părţilor aflate în conflict se execută din teritoriile proprii, din apele internaţionale, din spaţiul aerian internaţional şi, cu anumite limitări, din spaţiul cosmic. Executarea operaţiilor cibernetice de pe teritoriul altor state neimplicate în conflict este, în general, interzisă deoarece aceasta se face cu încălcarea suveranității statului respectiv. De asemenea, o importanţă deosebită în acest sens o are principiul neutralităţii deoarece operaţiile cibernetice, prin tranzitarea unui stat neutru, pot avea efecte neintenţionate în teritoriul acestuia.

În contextul războiului cibernetic, restricţiile bazate pe limitări geografice sunt extrem de dificil de aplicat. De pildă, putem considera situaţia în care un atac cibernetic este dezvoltat prin tehnici de *cloud computing*[4]. Datele utilizate pentru a orchestra un atac dintr-un stat pot fi replicate în alte state, inclusiv în state neutre, dar observabile doar în sistemele unde atacul a fost iniţiat şi finalizat. Nu există nicio interdicţie generală privind simpla tranzitare a datelor prin zone în care executarea operaţiilor cibernetice este în mod normal interzisă, în timpul unui conflict armat.

Conform concepţiei tradiţionale exprimată în legislaţia conflictelor armate, operaţiile militare executate în cadrul unui conflict armat cu caracter non-internaţional ar trebui să se limiteze la teritoriul, inclusiv marea teritorială şi spaţiul aerian naţional, al statului în care are loc conflictul[5]. Cu toate acestea, evenimentele din ultima perioadă, cum ar fi conflictul din Afganistan şi operaţiile transfrontaliere de combatere a terorismului, au evidenţiat dificultatea trasării unor astfel de limite. În prezent, domeniul geografic exact al conflictului armat cu caracter non-internaţional ridică o serie de probleme complexe, fiind supus, în acelaşi timp, unui anumit grad de controversă. De exemplu, unele state consideră că o confruntare armată non-internaţională se poate extinde dincolo de limitele frontierelor statului în cauză, argumentând că statutul actorilor, nu geografia, este factorul determinant în clasificarea conflictelor[6].

2. Tipuri de conflicte armate

Criteriile general acceptate pe baza cărora se stabileşte existenţa unui *conflict armat internaţional* derivă din prevederile art. 2 comun al Convenţiilor de la Geneva[7]. Astfel, o confruntare este internaţională în momentul în care două sau mai multe state sunt implicate în conflict. De asemenea, avem confruntare internaţională şi în situaţia în care un grup armat organizat, aflat sub controlul unui stat, se angajează în ostilităţi împotriva unui alt stat.

Controlul exercitat de către stat asupra forţelor armate subordonate sau a miliţiilor ori a unităţilor paramilitare poate avea un caracter global și trebuie să cuprindă mai mult decât simpla furnizare de sprijin financiar, echipament militar sau pregătire. Cu toate acestea, nu înseamnă că este obligatorie includerea emiterii ordinelor sau direcţiilor specifice fiecărei operaţii de către stat pentru dovedirea controlului. Potrivit dispoziţiilor dreptului internaţional, nu este în niciun caz necesar ca au-

torităţile statului să planifice toate operaţiile unităţilor care depind de ele, să le aleagă obiectivele sau să transmită instrucţiuni specifice privind desfăşurarea operaţiilor militare pentru a fi demonstrat controlul statului asupra respectivului actor non-statal. Ca atare, conform dreptului internaţional, controlul exercitat de stat poate fi considerat ca existând atunci când respectivul stat are rol în organizarea, planificarea şi coordonarea acţiunilor militare ale actorului non-statal, adiţional finanţării, instruirii şi echipării sau furnizării de sprijin operaţional acelui actor.

Raportându-ne la mediul virtual, dacă un stat exercită controlul global asupra unui grup de hackeri care angajează infrastructuri cibernetice ale altui stat şi provoacă pagube fizice semnificative, conflictul reprezintă un conflict armat internaţional. Statul care exercită controlul asupra grupului de hackeri nu trebuie să fi instruit membrii grupului să atace anumite facilități ale infrastructurilor cibernetice, fiind suficientă doar exercitarea controlului atât cât să-i îndrume pentru a lansa o campanie împotriva ţintelor cibernetice ale statului-victimă. Desigur, simpla susţinere a unui actor non-statal implicat într-un conflict armat non-internaţional nu-l transformă într-o confruntare internaţională. Cu alte cuvinte, sprijinul în sine nu transformă conflictul armat cu caracter non-internaţional într-un conflict armat internaţional între statul care oferă suport şi statul pe teritoriul căruia se desfăşoară conflictul, dacă statul care oferă sprijin actorului non-statal nu exercită controlul global asupra acestuia, această imixtiune putând fi totuşi catalogată ca o acţiune ilegală de intervenţie în afacerile interne ale statului pe teritoriul căruia se desfăşoară intruziunea.

Interpretarea prezentată mai sus, referitoare la existenţa controlului global al unui stat asupra actorului non-statal pentru ca faptele celui din urmă să fie atribuite şi statului, transformând astfel un conflict non-internaţional într-unul internaţional, a fost dată prima oară în anul 1999 de către Camera de Apel a Tribunalului internaţional pentru condamnarea persoanelor responsabile pentru încălcările grave ale dreptului internaţional umanitar comise începând cu anul 1991 pe teritoriul fostei Iugoslavii, cunoscut ca Tribunalul Penal Internaţional pentru fosta Iugoslavie[8].

În practică, este într-adevăr dificil de stabilit dacă acţiunile cibernetice ale unui actor non-statal sunt controlate de către un stat. Pentru a exemplifica cât de dificilă este probarea existenţei controlului unui stat asupra unui actor non-statal care acţionează în spaţiul cibernetic, vom lua, ca exemplu, operaţiile cibernetice desfăşurate împotriva Estoniei la nivelul anului 2007. Nu există dovezi clare care să ateste faptul că *hacktiviştii*[9] au executat operaţiile cibernetice conform instrucţiunilor vreunui stat şi nici că atitudinea acestora a fost aprobată şi adoptată de către un alt stat. Din aceste motive, situaţia din Estonia nu poate fi catalogată ca o confruntare armată internaţională.

Legislaţia conflictelor armate nu abordează în mod direct semnificaţia termenului de „conflict armat" însă, în mod evident, această noţiune solicită existenţa ostilităţilor militare, care presupun întrebuinţarea mijloacelor şi metodelor de război şi pot implica doar operaţii fizice sau cibernetice, precum şi orice combinaţii între acestea.

Aşadar ostilităţile militare sunt, fără îndoială, o condiţie precedentă a conflictului armat internaţional însă comunitatea internaţională nu a ajuns la un consens cu privire la pragul violenţei necesare. Spre exemplu, Comitetul Internaţional al Crucii Roşii, denumit în continuare CICR, consideră că orice divergenţă ivită între două sau mai multe state care conduce la intervenţia forţelor armate este o confruntare armată, fără a fi relevante durata conflictului sau numărul victimelor. În cadrul punctului 255 al comentariului din 2016 la art. 2 din Convenţia de la Geneva pentru îmbunătăţirea sorţii răniţilor şi bolnavilor din forţele armate în campanie[10], CICR apreciază că este general acceptat faptul că operaţiile cibernetice care au efecte similare cu operaţiile clasice cinetice pot constitui un conflict armat internaţional. Ca atare, dacă aceste operaţii duc la moartea sau rănirea militarilor, ori a civililor, sau la distrugerea bunurilor civile ori militare, nu ar exista niciun motiv pentru a trata speţa diferit faţă de atacurile cu repercusiuni echivalente executate prin metode şi mijloace de război tradiţionale. Mergând pe această logică, o operaţie cibernetică ce provoacă o explozie la o mică facilitate militară ar fi suficientă pentru încadrarea acțiunii într-un conflict armat internaţional.

Există şi opinii contrare, potrivit cărora este necesară o mai mare măsură, durată sau intensitate a ostilităţilor pentru ca acestea să intre în categoria conflictelor armate internaţionale. Christopher Greenwood se referă la cazul pilotului american al cărui avion a fost doborât deasupra Libanului în anii '80 de către forţele siriene, acesta fiind capturat. În viziunea SUA, incidentul a îndeplinit criteriile unui conflict armat și, ca atare, pilotului trebuia să i se recunoască statul de prizonier de război în baza dispozițiilor Convenţiei de la Geneva privitoare la tratamentul prizonierilor de război. Cu toate acestea el comentează că nu este obligatoriu ca statele să aibă întotdeauna o astfel de interpretare: „*Poate că numai atunci când ostilitățile ating un nivel de intensitate care depășește nivelul unor astfel de confruntări izolate, va fi tratat ca un conflict armat căruia i se aplică regulile DIU*"[11]. Deşi o astfel de opinie are rădăcini puternice în practica statelor, care demonstrează că de-a lungul timpului au existat o serie de incidente izolate cum ar fi ciocnirile sporadice în zona frontierelor sau incidentele navale care nu au condus la iniţierea unor con-

flicte armate, o astfel de teorie are un impediment major: nu se poate conveni asupra unui anumit prag care, odată atins, să ridice agresiunile la nivel de conflict armat internaţional. Astfel, un singur incident în mediul virtual care provoacă numai răniri, deces, distrugeri sau pagube nu ar determina neapărat o confruntare armată internaţională. De exemplu, cazul Stuxnet când, în 2010, o operaţie cibernetică executată împotriva sistemelor SCADA[12] ale unei instalaţii de îmbogăţire a uraniului din Iran au dus la deteriorarea fizică a centrifugelor acesteia, dar elementele de ordin juridic şi practic au limitat concluzionarea că atacul cibernetic a avut loc în cadrul unui conflict armat internaţional. De fapt, până în prezent, niciun conflict armat internaţional nu a fost declarat în mod public ca fiind cauzat de acţiuni dezvoltate în mediul virtual. Cu toate acestea, consider că operaţiile cibernetice au potenţialul de a depăşi magnitudinea unui conflict armat internaţional.

Conflictul armat cu caracter non-internaţional este o situaţie de violenţă armată intensă şi regulată între forţele de securitate ale unui stat, în special armata, şi unul sau mai multe grupări militare neguvernamentale organizate[13]. Conflict armat non-internaţional este şi atunci când există o situaţie de violenţă armată intensă între două sau mai multe forțe de securitate organizate dintr-un stat. Perturbările şi tensiunile interne, inclusiv revoltele sau actele de violenţă izolate şi sporadice, precum şi alte similare nu pot fi catalogate ca fiind conflicte armate.

Legislaţia internaţională privind conflictele armate vorbeşte despre conflictul armat non-internaţional, în primul rând, prin prisma dispoziţiilor art. 3 comun celor patru Convenţii de la Geneva din 12 august 1949[14], care reflectă dreptul internaţional cutumiar, dar şi prin prevederile art. 8 din Statutul Curţii Penale Internaţionale[15] care consideră drept crime de război violările grave ale art. 3 comun celor patru Convenţii.

Aplicarea legislaţiei conflictelor armate nu depinde de tipul operaţiilor militare sau de metodele şi mijloacele specifice conflictului în cauză. Prin urmare, simplele operaţii cibernetice, chiar și în absenţa operaţiilor militare fizice, pot crea un conflict armat cu caracter non-internaţional. Cu toate acestea, având în vedere magnitudinea violenţei şi gradul de organizare al grupurilor armate, necesare pentru ca o confruntare să fie ridicată la nivelul de conflict armat non-internaţional, doar în cazuri excepţionale operaţiile cibernetice în sine vor constitui o confruntare armată non-internaţională. Desigur, dacă un conflict este calificat drept confruntare armată cu caracter non-internaţional în virtutea operaţiilor militare fizice în desfăşurare, legislaţia care guvernează acest tip de conflicte va fi aplicabilă oricărei operaţii cibernetice executată în cadrul acestuia.

Există două tipuri de interpretări ale sintagmei „ivit pe teritoriul uneia dintre Înaltele Părţi Contractante” din cuprinsul art. 3 comun celor patru Convenţii. O primă interpretare ar putea fi că „uneia” din fraza citată restricţionează conflictele armate non-internaţionale în limitele teritoriale ale unui singur stat. O astfel de interpretare transformă orice confruntare armată care traversează graniţele într-un conflict armat internaţional. O a doua interpretare ar fi că „uneia” reprezintă o referire la teritoriul oricăreia dintre Înaltele Părţi Contractante. În consecinţă, expresia nu impune limitări teritoriale atât timp cât toate statele suverane relevante sunt părţi ale Convenţiilor de la Geneva. Astfel, dacă un atac cibernetic este întreprins în timpul unui conflict armat non-internaţional, din afara teritoriului statului, nu înseamnă că acest aspect va „internaţionaliza” conflictul. Trebuie să precizez că achiesez la această interpretare, în special din perspectiva mediului virtual, ţinând cont că tranzitul de date prin intermediul infrastructurilor cibernetice situate în afara statului în care se desfăşoară conflictul armat non-internaţional nu îl transformă într-un conflict armat internaţional. Mai mult, trebuie avut în vedere faptul că operaţiile cibernetice executate în cadrul unui conflict armat non-internaţional pot fi lansate de la distanţă, departe de zona în care se desfăşoară ostilităţile. Unele state au cadre normative insuficient dezvoltate în ceea ce priveşte activităţile din spaţiul cibernetic sau nu au capacitatea, din punct de vedere tehnic, de a controla eficient activităţile cibernetice care au loc pe teritoriul lor. Acestea constituie un punct de atracţie pentru grupările implicate în atacuri cibernetice în timpul unui conflict armat non-internaţional.

Aşa cum am precizat mai sus, situaţiile de perturbări şi tensiuni interne, cum ar fi revoltele, actele de violenţă izolate şi sporadice precum şi alte acte de natură similară nu se ridică la nivelul de conflicte armate non-internaţionale. Interpretarea se întemeiază pe dispoziţiile art. 1 alin. (2) din Protocolul adiţional II la Convenţiile de la Geneva din 12 august 1949 privind protecţia victimelor conflictelor armate fără caracter internaţional[16]. Raportând aceste prevederi la spaţiul virtual, incidentele cibernetice sporadice, inclusiv cele care provoacă daune materiale sau victime ori cele care instigă la tulburări domestice sau terorism intern, nu se ridică la nivelul de conflict armat non-internaţional. Cu titlu de exemplu, apelurile pentru revolte făcute în spaţiul cibernetic de către minoritatea rusă din Estonia, în 2007, nu pot fi considerate ca îndeplinind pragul unui conflict armat cu caracter non-internaţional.

Ca atare, elementele-cheie ale unui conflict armat non-internaţional sunt reprezentate de intensitatea ostilităţilor şi implicarea unui grup armat organizat. Criterii orientative care să faciliteze determinare atingerii pragului de conflict armat cu caracter non-internaţional într-o anumită situaţie sunt: gravitatea atacurilor şi repartiţia acestora; dacă vio-

lenţele fac obiectul unui control sau a unei alte acţiuni relevante ale Consiliului de Securitate al ONU; extinderea temporală şi teritorială a violenţelor şi caracterul colectiv al ostilităţilor; creşterea numărului forţelor guvernamentale; dacă părţile la conflict pot opera dintr-un teritoriu aflat sub controlul lor; mobilizarea voluntarilor, distribuţia şi tipul de arme utilizate de părţile la conflict; dacă înfruntarea a dus la o deplasare în masă a oamenilor. Având în vedere aceste criterii, putem afirma fără să greşim că rareori operaţiile cibernetice pot declanşa o confruntare armată non-internaţională.

3. Răspunderea penală pentru infracţiuni de război

Din multitudinea de forme de răspundere juridică consfinţite, alături de răspunderea disciplinară, contravenţională şi civilă, răspunderea penală este cea care produce cele mai serioase consecinţe asupra persoanei. Răspunderea penală constă în raportul juridic penal care ia fiinţă în urma săvârşirii unei infracţiuni[17].

Codul penal al României împarte infracţiunile de război în cinci mari categorii: infracţiuni de război contra persoanelor, infracţiuni de război contra proprietăţii şi altor drepturi, infracţiuni de război contra operaţiunilor umanitare şi emblemelor, utilizarea de metode interzise în operaţiunile de luptă şi utilizarea de mijloace interzise în operaţiunile de luptă. Pe scurt, încălcările grave ale legislaţiei conflictelor armate reprezintă crime de război şi implică răspunderea penală individuală.

Întrucât legislaţia conflictelor armate se aplică şi noilor metode şi mijloace de război, inexistente la momentul apariţiei normelor, actele săvârşite prin mijloace cibernetice care au efectele prevăzute de lege pot fi considerate crime de război. Interpretarea este valabilă deopotrivă în cazul membrilor forţelor armate şi civililor implicaţi în operaţii cibernetice executate în contextul conflictului armat, internaţional sau cu caracter non-internaţional, ori asociate acestuia. Nu pot fi acuzate de crime de război persoanele care sunt implicate în operaţii cibernetice pur infracţionale sau în activităţi necorespunzătoare în spaţiul virtual care nu au legătură cu conflictul armat, acţiunile acestora intrând, de la caz la caz, în categoria infracţiunilor contra siguranţei şi integrităţii sistemelor şi datelor informatice, falsurilor informatice, fraudelor comise prin sisteme informatice etc.

În ceea ce priveşte săvârşirea infracţiunilor de război prin operaţii cibernetice, acestea sunt de trei feluri: săvârşirea în calitate de unic autor, săvârşirea în comun cu alte persoane (coautorat şi/sau complicitate)[18] şi săvârşirea prin intermediul altor indivizi. De asemenea, tentativa la infracţiunile de război se pedepseşte.

În context cibernetic, o persoană răspunde penal atunci când, prin intermediul unei operaţii cibernetice, comite un act interzis de lege. Termenul „comite" se referă la săvârşirea fizică a unei infracţiuni sau a unei omisiuni care încalcă legea penală. Spre exemplu, un membru al forţelor armate responsabil cu executarea operaţiilor cibernetice, pe timpul unui conflict armat, accesează sistemul de control al unei centrale electrice oprind furnizarea energiei electrice către o localitate situată pe teritoriul adversarului. Presupunând că încălzirea localităţii respective se face exclusiv prin energie electrică, iar atacul se desfăşoară iarna, rezultă victime în rândul populaţiei civile. Nici centrala şi nici populaţia localităţii nu sunt obiective militare, prin urmare operatorul poate fi tras la răspundere pentru săvârşirea unei infracţiuni de război.

Răspunderea penală individuală pentru crime de război poate fi angajată şi prin omisiune, acolo unde legislaţia conţine o obligaţie de a acţiona. O importanţă deosebită în această circumstanţă este responsabilitatea superiorilor şi comandanţilor de a preveni executarea oricărei operaţii cibernetice care se califică drept infracţiune de război.

Crimele de război prin mijloace cibernetice pot fi, de asemenea, săvârşite şi prin coautorat sau complicitate atunci când un individ acţionează în comun cu alţii potrivit unui plan sau scop comun. Ca atare, contribuţiile persoanelor implicate trebuie să facă parte dintr-un plan comun sau acord, iar coautorii sau complicii trebuie să contribuie în mod coordonat la comiterea faptelor ce constituie infracţiuni de război. Nu este obligatoriu ca aceste contribuţii să aibă loc doar în faza de execuţie sau exclusiv în această fază, ele putând fi conturate şi în faza planificării şi pregătirii operaţiei. Nici făptuitorul nu trebuie să fie prezent la locul săvârşirii infracţiunii atât timp cât, împreună cu ceilalţi, a exercitat controlul asupra acesteia. Răspunderea penală în astfel de circumstanţe este deosebit de relevantă din punctul de vedere al mediul virtual, deoarece interconectivitatea specifică domeniului cibernetic oferă un mediu aproape ideal pentru faptele săvârşite în comun de diverşi autori. De pildă, un exemplu de coautorat ar fi atunci când specialişti din cadrul structurii de comunicaţii şi informatică a unui serviciu de informaţii dezvoltă un *malware*[19] destinat să afecteze sistemele de control ale traficului rutier din statul advers, provocând o serie de accidente grave. Deşi *malware*-ul este implantat în cadrul unei operaţii executată de structura operativă a respectivului serviciu de informaţii, specialiştii ambelor structuri vor răspunde penal pentru încălcarea legislaţiei conflictelor armate.

Răspunderea penală pentru acţiunile executate prin intermediul altor persoane poate fi, la rândul ei, de două feluri: prin instigare, atunci când o persoană determină, cu intenţie, o altă persoană să comită o infracţiune, sau când un superior ordonă unui subordonat să se angajeze într-o operaţie care constituie infracţiune de război. Bineîn-

ţeles că, în situaţia în care subordonatul are toate elementele la dispoziţie pentru a-şi da seama că operaţia constituie o încălcare a legislaţiei, acesta este obligat să n-o execute[20]. În mediul virtual însă, este, de cele mai multe ori, extrem de dificil ca executantul unei operaţii cibernetice să ia în calcul toate efectele unei astfel de operaţii ori, în acest caz, când subordonatul nu-şi poate da seama şi nu dispune de elementele necesare pentru a realiza faptul că operaţia pe care o execută e calificată drept infracţiune de război, iar superiorul, din poziţia sa, dispune de aceste elemente, cel din urmă va purta întreaga răspundere penală.

Cu privire la sancţionarea tentativei în cazul infracţiunilor de război, aşa cum am precizat mai sus, aceasta se pedepseşte, cel puţin la nivel naţional, în temeiul prevederilor art. 445 din Codul Penal al României. La nivel internaţional, tentativa în cazul infracţiunilor de război este sancţionată prin prisma dispoziţiilor art. 25 alin. (3) lit. f) din Statutul Curţii Penale Internaţionale care prevede că o persoană răspunde penal şi poate fi pedepsită pentru o crimă ce ţine de competenţa Curţii dacă: „încearcă să comită o asemenea crimă prin acte care, prin caracterul lor substanţial, constituie începutul executării crimei fără ca aceasta să fie îndeplinită datorită unor circumstanţe independente de voinţa sa […]". Aşadar, având în vedere prevederile menţionate, este clar că noţiunea de tentativă de săvârşire a infracţiunilor de război este aplicabilă şi în cazul operaţiilor cibernetice.

Concluzii

Problematica aplicării legislației conflictelor armate în contextul operațiilor desfășurate în mediul virtual este una foarte delicată. Prin prezenta lucrare am încercat abordarea acesteia pe trei mari planuri: contextul geografic, tipurile de conflicte armate – internaționale sau non-internaționale – și răspunderea penală pentru infracțiunile de război.

Astfel, dacă în operațiile tradiționale delimitarea geografică nu solicită un efort prea mare, în cazul operațiilor cibernetice situația se complică. Așa cum am prezentat mai sus, în cazul unui atac cibernetic desfășurat prin tehnici de *cloud computing,* datele utilizate dintr-un stat pot fi replicate în alte state, inclusiv în state neutre, dar observabile doar în sistemele unde atacul a fost iniţiat şi finalizat.

Referitor la tipurile de conflicte armate, din perspectivă cibernetică avem un conflict armat internaţional ori de câte ori există ostilităţi militare între două sau mai multe state care pot include sau se limitează doar la operaţii cibernetice. Referitor la conflictele armate non-internaționale, existența acestora în context cibernetic poate fi pusă în discuție ori de câte ori avem de-a face cu violenţă armată prelungită, care poate include sau se limitează doar la operaţii cibernetice, între forţele guvernamentale şi grupurile militare organizate sau între astfel de grupuri pe teritoriul unui singur stat. Confruntarea trebuie să atingă un nivel minim de intensitate, iar părţile implicate în conflict trebuie să aibă un grad minim de organizare.

În final, având în vedere faptul că operaţiile cibernetice se pot constitui în infracţiuni de război, rezultă că acestea, în mod logic, pot atrage răspunderea penală individuală.

Note bibliografice:

[1] *Convenţia de la Geneva (I) pentru îmbunătăţirea sorţii răniţilor şi bolnavilor din forţele armate în campanie, Convenţia de la Geneva (II) pentru îmbunătăţirea sorţii răniţilor, bolnavilor şi naufragiaţilor forţelor armate pe mare, Convenţia de la Geneva (III) privitoare la tratamentul prizonierilor de război, Convenţia de la Geneva (IV) privitoare la protecţia persoanelor civile în timp de război*, Geneva, 12 august 1949.

[2] *Protocolul adiţional I la Convenţiile de la Geneva privind protecţia victimelor conflictelor armate internaţionale* şi *Protocolul adiţional II la Convenţiile de la Geneva privind protecţia victimelor conflictelor armate fără caracter internaţional*, Geneva, 10 iunie 1977.

[3] *Convenția referitoare la legile și obiceiurile războiului terestru*, Haga, 18 octombrie 1907.

[4] *Cloud computing* reprezintă un ansamblu de stocare de date, aplicaţii, acces la informaţii şi servicii de calcul, livrat utilizatorului ca un serviciu, printr-o conexiune de reţea, fără ca acesta să cunoască amplasamentul şi configuraţia fizică a sistemelor care furnizează aceste servicii. Se bazează pe partajarea unor resurse fizice sau virtuale (software sau hardware), eludând necesitatea de avea acele resurse în posesia utilizatorului.

[5] Această interpretarea rezultă din analiza logică a art. 3 comun celor 4 Convenții de la Geneva: dacă un conflict armat fără caracter internațional depășește teritoriului statului în care s-a ivit, atunci se transformă într-un conflict armat internațional.

[6] ***, *Department of Defense Law of war manual*, Office of General Counsel Department of Defense, Washington, June 2015 (Updated December 2016), p. 73.

[7] Respectivul articol stipulează că „În afara dispoziţiilor care trebuie să intre în vigoare încă din timp de pace, prezenta convenţie se va aplica în caz de război declarat sau de orice alt conflict armat, ivit între două sau mai multe dintre Înaltele Părţi Contractante, chiar dacă starea de război nu e recunoscută de una din ele. Convenţia se va aplica, de asemenea, în toate cazurile de ocupaţie totală sau parţială a teritoriului unei Înalte Părţi Contractante, chiar dacă această ocupaţie nu întâmpină nici o rezistenţă militară. Dacă una dintre Puterile în conflict nu e parte la prezenta convenţie, Puterile care sunt părţi la aceasta vor rămâne totuşi legate prin ea în raporturile lor reciproce. În afară de aceasta, ele vor fi legate prin convenţie faţă de sus-zisa Putere, dacă aceasta o acceptă şi îi aplică dispoziţiile".

[8] *Prosecutor v. Duško Tadic*, Case No.: IT-94-1-A, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, 15 July 1999, URL: http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf, accesat la 06.07.2018.

[9] *Hacktivismul* reprezintă folosirea unui calculator, a unei rețele de calculatoare sau a oricărui alt sistem IT&C pentru a promova, susține și dezbate o cauză politică.

[10] *Commentary of 2016 Article 2: Application of the Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, International Committee of the Red Cross, Geneva, 12 august 1949, URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518, accesat la 07.07.2018.

[11] Christopher Greenwood, "Scope of application of humanitarian law" în Dieter Fleck (ed.), *The handbook of international humanitarian*

law, Second Edition, Oxford, 2008, p. 45.

[12] Termenul SCADA (*Supervisory Control and Data Acquisition*) se referă de obicei la un centru de comandă care monitorizează și controlează un întreg spațiu de producție. Funcțiile de control ale centrului de comandă sunt, în majoritatea cazurilor, restrânse la funcții decizionale sau funcții de administrare generală.

[13] Această definiţie a fost dată de către Camera de apel a Tribunalului Penal Internaţional pentru fosta Iugoslavie în *Decizia privind propunerea de apărare pentru recursul interlocutoriu privind competenţa* din 02 octombrie 1995, pct. 70 (Prosecutor vs. Duško Tadic), URL: http://www.icty.org/x/cases/tadic/acdec/en/51002.htm, accesat la 08.07.2018.

[14] Respectivul articol stipulează că „În caz de conflict armat neprezentând un caracter internaţional şi ivit pe teritoriul uneia dintre Înaltele Părţi Contractante, fiecare dintre Părţile în conflict va trebui să aplice cel puţin următoarele dispoziţii: persoanele care nu participă direct la ostilităţi, inclusiv membrii forţelor armate care au depus armele şi persoanele care au fost scoase din luptă din cauză de boală, rănire, detenţiune sau din orice altă cauză, vor fi, în toate împrejurările, tratate cu omenie, fără nici o deosebire cu caracter discriminatoriu bazată pe rasă, culoare, religie sau credinţă, sex, naştere sau avere sau orice alt criteriu analog […]”.

[15] *Statutul Curţii Penale Internaţionale*, Roma, 17 iulie 1998, URL: http://legislatie.just.ro/Public/DetaliiDocument/34774, accesat la 08.07.2018.

[16] Respectivul articol stipulează că „Prezentul Protocol nu se va aplica situaţiilor de tensiune internă şi tulburărilor interne cum sunt actele de dezordine publică, actele sporadice şi izolate de violenţă şi alte acte analoge, care nu sunt conflicte armate”.

[17] Potrivit dispoziţiilor art. 15 alin. (1) din Codul Penal al României, „infracţiunea este fapta prevăzută de legea penală, săvârşită cu vinovăţie, nejustificată şi imputabilă persoanei care a săvârşit-o”.

[18] Coautorii sunt persoanele care comit nemijlocit aceeaşi infracţiune – art. 46 alin. (2) din Codul Penal al României, în timp ce complicele este persoana care, cu intenţie, facilitează sau ajută o altă persoană să comită o infracţiune ori îi promite acesteia că va ascunde bunurile provenite din faptă sau că o va favoriza – art. 48 din respectivul Cod.

[19] *Malware* (*Malicious Software*) sau software rău-intenționat este un program proiectat cu scopul de a accesa și/sau deteriora un computer și/sau o rețea de computere fără consimțământul proprietarului.

[20] Art. 8 lit. b) din *Legea nr. 80/1995 privind Statutul cadrelor militare* stipulează că „[…] Cadrelor militare nu li se poate ordona şi le este interzis să execute acte contrare legii, obiceiurilor războiului şi convenţiilor internaţionale la care România este parte […]”, iar art. 5 lit. d) din *Legea nr. 384/2006 privind Statutul soldaţilor şi gradaţilor profesionişti* că „[…] Soldaţilor şi gradaţilor profesionişti nu li se poate ordona şi le este interzis, în orice situaţie, să execute acte contrare legii, obiceiurilor războiului şi convenţiilor internaţionale la care România este parte […]”.

Bibliografie selectivă:

Convenții, tratate și protocoale internaționale, legi și hotărâri ale Parlamentului României, precum și ordine ale instituțiilor și autorităților publice:

a) *Carta Națiunilor Unite*, San Francisco, 26 iunie 1945;
b) *Convenția referitoare la legile și obiceiurile războiului terestru*, Haga, 18 octombrie 1907;
c) *Convenţia de la Geneva (I) pentru îmbunătăţirea sorţii răniţilor şi bolnavilor din forţele armate în campanie*, Geneva, *Convenţia de la Geneva (II) pentru îmbunătăţirea sorţii răniţilor, bolnavilor şi naufragiaţilor forţelor armate pe mare*, *Convenţia de la Geneva (III) privitoare la tratamentul prizonierilor de război* și *Convenţia de la Geneva (IV) privitoare la protecţia persoanelor civile în timp de război*, Geneva, 12 august 1949;
d) *Protocolul adiţional I la Convenţiile de la Geneva privind protecţia victimelor conflictelor armate internaţionale* și *Protocolul adiţional II la Convenţiile de la Geneva privind protecţia victimelor conflictelor armate fără caracter internaţional*, Geneva, 10 iunie 1977;
e) *Statutul Curţii Penale Internaţionale*, Roma, 17 iulie 1998;
f) *Tratatul Organizației Atlanticului de Nord,* Washington DC, 4 aprilie 1949;
g) *Tratatul privind Uniunea Europeană și Tratatul privind Funcționarea Uniunii Europene*;
h) *Convenția Consiliului Europei privind criminalitatea informatică*, Budapesta, 23 noiembrie 2001;
i) *Protocolul adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice*, Strasbourg, 28 ianuarie 2003;
j) *Legea nr. 105/2009 pentru ratificarea Protocolului adițional la Convenția privind criminalitatea informatică*;
k) *Hotărârea Guvernului nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național pentru implementarea Sistemului național de securitate cibernetică*;
l) *Legea nr. 80/1995 privind statutul cadrelor militare*;
m) *Legea nr. 384/2006 privind Statutul soldaţilor şi gradaţilor profesionişti*.

Lucrări de specialitate:

a) ***, *Department of Defense, Law of war manual*, Office of General Counsel Department of Defense, Washington, June 2015;
b) ***, *Dicționarul Explicativ al limbii române*, ediția a II-a, Editura Universul enciclopedic, 1998;
c) BALOG,Cătălin-Iulian, *Managementul riscurilor de securitate în spațiul cibernetic cu aplicații în domeniul militar*, București, 2016;
d) DAN-ȘUTEU, Ștefan-Antonio, *Procedee, tehnici și metode de integrare a apărării cibernetice în operația militară*, București, 2016;
e) GREENWOOD, Christopher, “Scope of application of humanitarian law” în Dieter Fleck (ed.), *The handbook of international humanitarian law*, Second Edition, Oxford, 2008;
f) STARR Stuart; WENTZ, Larry K., *Cyberpower and National Security*, Washington DC, National Defense University Press, Potomac Books, 2009.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 1913/2018

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Site: https://cssas.unap.ro